Проблемы оценки соответствия в информационных технологиях

Ю.И. Иванченко

В докладе представлен краткий анализ нормативных правовых актов РБ касающихся обеспечения ИБ и оценки соответствия объектов ИТ требованиям по ИБ.

В настоящих тезисах представлены положения нормативных правовых актов Республики Беларусь, которые, по мнению автора, являются проблемными и требуют обсуждения на профессиональном уровне.

Ключевым нормативным правовым актом в рассматриваемой области является Закон Республики Беларусь «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации». Он определяет терминологию, правовые и организационные основы оценки соответствия объектов оценки требованиям **только технических** нормативных правовых актов.

Оценка соответствия определяется как деятельность по определению соответствия объектов оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации. К техническим нормативным правовым актам в области технического нормирования и стандартизации относятся [2]:

технические регламенты;
технические кодексы;
стандарты, в том числе государственные стандарты, стандарты организаций;
технические условия.

Цели оценки соответствия определены в статье 5 [1] и включают:

- обеспечение защиты жизни, здоровья и наследственности человека, имущества и охрану окружающей среды;
- повышение конкурентоспособности продукции (работ, услуг);
- обеспечение энерго- и ресурсосбережения;
- создание благоприятных условий для обеспечения свободного перемещения продукции на внутреннем и внешнем рынках, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле.

Виды оценки соответствия установлены в статье 7 [1] и включают всего 2 вида: аккредитацию и подтверждение соответствия. Подтверждение соответствия (статья 25) может носить обязательный или добровольный характер. Обязательное подтверждение соответствия осуществляется в форме обязательной сертификации и декларирования соответствия. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Объекты оценки соответствия по каждому виду оценки определены в статье 8 [1]:

- *при аккредитации* это компетентность юридического лица в выполнении работ по подтверждению соответствия или проведении испытаний объектов оценки соответствия.
- *при подтверждении соответствия это*:

продукция и процессы ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации;
выполнение работ и оказание услуг;
системы управления качеством;
системы управления окружающей средой;
системы управления безопасностью продукции;
системы управления охраной труда;
профессиональная компетентность персонала в выполнении определенных работ (оказании определенных услуг);
иные объекты, в отношении которых установлены требования технических нормативных правовых актов. К техническим нормативным правовым актам в области технического нормирования и стандартизации, на соответствие требованиям которых осуществляется

оценка соответствия, относятся технические регламенты и государственные стандарты Республики Беларусь.

В тоже время закон Республики Беларусь «О техническом нормировании и стандартизации» к объектам технического нормирования, объектам стандартизации относит только продукцию, процессы ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказание услуг.

В законе «Об информации, информатизации и защите информации» введены 2 понятия – аттестация и государственная экспертиза в следующем контексте (без определений).

«Информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должны обрабатываться в информационных системах с применением системы защиты информации, **аттестованной** в порядке, установленном Советом Министров Республики Беларусь».

«Для создания системы защиты информации используются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам **государственной экспертизы**, порядок проведения которой определяется Советом Министров Республики Беларусь». Т.о. по букве закона оба этих понятия остаются за рамками **Национальной системы подтверждения соответствия.**

Что такое система защиты информации в законе не уточняется, но определены меры по защите информации, которые, по-видимому, должны быть реализованы в упомянутой системе.

К правовым мерам по защите информации отнесены заключаемые **обладателем** информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации отнесены меры обеспечения особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим (программно-техническим) мерам по защите информации отнесены меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Положением о порядке аттестации **систем защиты информации** [3] аттестация определяется как комплекс организационно-технических мероприятий, в результате которых **подтверждается соответствие** системы защиты информации требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, и оформляется аттестатом соответствия. Система защиты информации определена как совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, функционирующих по правилам, установленным соответствующими нормативными правовыми актами в области защиты информации, в том числе техническими нормативными правовыми актами. Таким образом, Положение расширяет установленный законом [1] перечень форм подтверждения соответствия.

Указом Президента Республики Беларусь «О лицензировании отдельных видов деятельности» от 01.09.2010 №450 в дополнение к существовавшим видам деятельности, на осуществление которых требуются специальные разрешения (лицензии) введены еще два: аттестация объектов информатизации и аттестация информационных систем, но не систем защиты информации.

В Положении содержится исчерпывающий перечень того, что в себя включает оценка системы защиты информации:

анализ организационной структуры информационной системы, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения системы защиты информации, разработанной документации и ее соответствия требованиям нормативных правовых актов в области защиты информации (!?), в том числе технических нормативных правовых актов.

проверку правильности отнесения информационной системы к классу типовых объектов информатизации, выбора и применения средств защиты информации;

рассмотрение и анализ результатов испытаний средств защиты информации и системы защиты информации;

проверку уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

оценку системы защиты информации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

оформление протоколов испытаний (оценки) и заключения по результатам проверок.

В перечне исходных данных из 21 позиции, в частности, указаны документы, устанавливающие отнесение информационной системы к классу типовых объектов информатизации согласно СТБ 34.101.30-2007 и Задание по безопасности на информационную систему (вопрос разработки Задания по безопасности на информационную систему (даже как совокупность банков данных, информационных технологий и комплексов программно-технических средств) заслуживает отдельного обсуждения). Сам стандарт определяет объекты информатизации как средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с программным обеспечением, которые используются для обработки информации. Встает вопрос о корректности и применимости СТБ 34.101.30 при проведении аттестации. Оценка же системы защиты информации на соответствие Заданию по безопасности на информационную систему видимо предполагается в процессе «проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации».

Положение игнорирует СТБ ISO/IEC 27001, содержащий требования именно к системам, и политику безопасности, хотя «Положение о порядке защиты информации …» требует разработки (актуализации) политики информационной безопасности.

Литература

1. Закон Республики Беларусь «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации».

2. Закон Республики Беларусь «О техническом нормировании и стандартизации».

3. Постановление Совета Министров Республики Беларусь 26 мая 2009, №675 О некоторых вопросах защиты информации.